경영학석사 학위논문

네트워크 가외성이 비즈니스 네트워크 견고성에 미치는 영향에 대한 연구

– 기업 데이터 네트워크를 중심으로 –

The Effects of Network Redundancy on the Resilience of Business Network: Focusing on the Firm Data Network

2017년 2월

서울대학교 대학원

경영학과 전략 전공

정다운

초 록

이 논문은 인터넷의 등장과 함께 많은 기업들이 전통적인 사업 영역에서는 경험할 수 없었던 새로운 종류의 위기인 인터넷 상에서의 사이버 공격으로부터 기업의 정보 자산(information assets)을 보호하기 위한 네트워크 견고성을 제고하는 전략을 주요 주제로 하고 있다. 보안 침입은 직접적으로 기업의 데이터 네트워크에 침투하여 기업의 주요 정보 자산을 유출시킬 뿐 아니라, 일시적으로 기업의 서버를 마비시켜 서비스를 정지시키며 직접적인 재무적 손실을 일으킨다. 이를 통해 기업이 입을 수 있는 직접적인 피해의 규모도 크지만, 이후 그 사실이 시장에 밝혀질 경우 후속적으로 기업의 시장 가치가 하락한다는 사실 또한 기업의 장기적인 생존에 중대한 영향을 미칠 수 있다. 이에 본 논문은 기업 데이터 네트워크를 중심으로 네트워크 가외성(network redundancy)을 추가하여 오류 및 공격 상황에서 기업의 피해 규모를 줄일 수 있는 장치에 대한 연구를 시뮬레이션 연구 방법론을 통해 진행한다. 우리는 이 연구 결과를 바탕으로 트라이어드 형성(triad formation)이라는 비교적 단순한 장치가 기업들이 이용하는 네트워크 서비스의 견고성을 제고하기 위한 실현 가능하고 유용한 해결책이 될 수 있음을 제시한다.

주요어 : 네트워크 가외성, 비즈니스 네트워크, 네트워크 견고성

학 번 : 2015-20666

목 차

표 목차

그림 목차

제 1 장 서 론

제 1 절 연구의 배경

인터넷의 등장과 함께 많은 기업들이 전통적인 사업 영역에서는 경험할 수 없었던 새로운 종류의 위기에 직면하고 있다. 그 중 대표적인 하나가 바로 인터넷 상에서의 사이버 공격으로부터 기업의 정보 자산(information assets)을 보호하는 일이다 (Hovav et al, 2003). 2000년대 이후 기업들의 컴퓨터와 인터넷에 대한 사업 의존도가 갈수록 높아지고 있는 실정이며, 이와 관련한 위험(risk)는 미국과 유럽의 하이테크 기업 경영자들을 상대로 한 경영 상의 우려에 관한 설문에서 각각 1, 2위를 기록한 바 있다(Salierno, 2001). 이토록 기업의 정보 자산 보호에 대한 관심이 대두된 주요 이유는 바로 보안 침입(security breach)이 기업 성과(performance) 직간접적인 악영향을 미치기 때문이다 (Warren et al., 2000; Glover et al., 2001; Kannan et al., 2007).

보안 침입은 다양한 목적을 지니며, 그에 따라 여러 형태로 발생할 수 있다. 직접적으로 기업의 데이터 네트워크에 침투하여 기업의 주요 정보 자산을 유출시키는 형태의 보안 침입뿐 아니라, 일시적으로 기업의 서버를 마비시켜 서비스를 정지시키는 형태의 보안 침입도 존재한

다. 이를 통해 기업이 입을 수 있는 직접적인 피해의 규모도 크지만, 이후 그 사실이 시장에 밝혀질 경우 후속적으로 기업의 시장 가치가 하락한다는 사실 또한 기업의 장기적인 생존에 중대한 영향을 미칠 수 있다 (Campbell et al., 2003; Hovav et al., 2003; Cavusoglu et al., 2004). 실제로 2004년 카셸(Cashell)에 의해 진행된 연구에 따르면 보안 침입의 타겟 기업(target firm)은 침입 이후 평균적으로 1-5% 수준의 주가 하락을 기록하는 것으로 밝혀졌으며, 이는 당시의 NYSE(New York Stock Exchange) 기준 500억-2000억원 규모의 주주 가치 손실로 해석된다 (Cashell et al., 2004).

2000년대 이후 발생한 수백 수천건의 보안침입과 그에 따른 기업들의 피해 사례 또한 이 사안의 심각성을 보여준다. 지난 10여년 간 소니(Sony), 아마존(Amazon), 애플(Apple), 페이스북(Facebook), 트위터(Twitter), 페이팔(PayPal) 등 수많은 대형 IT 기업들이 보안 침입의 피해에 노출되었다. 가장 대표적인 사례가 바로 소니로, 2011년과 2014년 각기 플레이스테이션 게임 부문과 엔터테인먼트 부문의 네트워크에 대한 보안 침입으로 큰 타격을 입은 바 있다. 소니는 2번의 보안 침입을 통해 직원 개인 정보와 사내 이메일, 내부 인사망 및 급여 체계, 미개봉 게임 및 영화 파일 등의 기업 주요 정보를 유출 당했고, 이를 통해 총 3000억원 규모의 피해를 기록하였다. 이처럼 소니와 같은 첨단 제조업체는 직접적인 기업 정보가 외부로 유출되는 것으로 큰 타격을 입을 수 있으나, 그 대상을 전자상거래 기업의 경우로 확대해보면 문제는 더욱 심각해질 수 있다. 전자상거래 기업의 서비스 마비는 사업 자체의 마비와 직결되는 까

닭이다. 2015년 아마존의 일일 매출액은 3500여억원으로 알려져 있으며, 24시간 동안 동질적으로 매출이 발생한다고 가정하더라도 몇 시간의 서비스 마비를 통해 아마존이 입을 수 있는 피해 규모는 수백억원에 달한다. 실제로 아마존은 일일 매출액 규모가 2015년의 1/10 규모에 지나지 않던 2008년 DDoS 공격으로 인해 2시간 동안 서비스가 마비되었던 적이 있으며, 이를 통해 총 42억원의 직접적인 손실을 기록한 바 있다. 한 데이터 침입 비용에 관한 연구에서는 2014년 미국 기업들이 보안 침입으로 인해 입은 평균 직접 손실은 회당 70억원 규모로 알려져 있으며, 국제적으로 보안 침입으로 인해 기업들이 입은 손실의 총 규모는 470조원에 달하는 것으로 밝혀졌다 (Ponemon Institute, 2014).

제 2 절 연구의 목적

2016년, 삼성 전자가 클라우딩 컴퓨팅 서비스 기업 조이언트(Joyent)를 인수한 것은 기업들의 네트워크 서비스에 대한 의존도가 더욱 심화되고 있음을 알려주는 신호탄 역할을 한다. 삼성의 조이언트 인수는 더 이상 기존의 아마존 웹 서비스(Amazon Web Service) 등의 외부 클라우딩 서비스에 의존하지 않고, 자체적인 네트워크 서비스 운영을 통해 고객 및 금융 정보를 관리하고 이를 통해 더욱 독자적인 성과를 확보하고자 하는 의지를 보여준다. 외부 서비스를 고용하는 것으로 끝나지 않고

자체적인 네트워크 서비스에 대한 의존도가 갈수록 심화되고 있는 이 시점에서, 기업이 자신이 기반한 네트워크의 본질적인 특성과 토폴로지 정확하게 이해하는 것은 올바른 대응 전략을 수립하는 데 있어 무엇보다 중요한 문제 중 하나이다.

현대 자동차 또한 커넥티드 카(connected car) 시대의 개막을 통해 클라우드 네트워크의 중요성에 주목하여 다양한 투자를 하기 시작한 사실은, 기존의 IT 기업들뿐 아니라, 전통적인 사업 영역에 속한 기업들 또한 네트워크의 중요성에 더욱 주목하기 시작했다는 사실을 보여준다. 그만큼 보안 침입이 기업의 성과에 미치는 영향의 심각성 또한 증가하고 있으나, 아직 이에 대한 경영자들의 인식 수준은 미비한 실정이다. 또한, 갈수록 다변화되는 보안 침입에 효과적으로 대응하는 전략을 수립하기 위해서 기업의 데이터 네트워크의 역학에 대한 이해 및 이와 관련된 연구가 필요하나, 이 역시 미흡한 상황이다. 기업들이 의존하는 네트워크 서비스는 자연스럽게 스케일 프리 네트워크(scale-free network)를 따라가는 것으로 밝혀졌으나, 전략 문헌에서 이를 접목한 연구는 아직 많지 않다. 따라서 본 논문에서는 기업이 보안 침입 상황에 대응하는 견고한 네트워크 아키텍처(network architecture)를 구성하기 위하여 어떠한 전략을 수립해야 하는가를 밝히고, 경영의 제반 이슈들에의 적용점을 찾기 위해 진행되었다.

제 2 장 이론적 배경과 가설의 설정

제 1 절 네트워크 이론과 전략 연구의 접점

기업의 정보가 구성되고 교환되는 네트워크 토폴로지(network topology)를 정확하게 이해하지 않고서는 외부 환경의 변화로 인한 영향과 양상을 제대로 분석하기 어렵다. 이렇듯 토폴로지의 관점에서 정보의 흐름을 파악하는 것은 물리적 시스템(e.g. 인터넷)과 사회적 시스템(e.g. 기업)의 커뮤니케이션, 조직화, 그리고 문제 해결의 측면에서 핵심적인 요소이나, 현실은 아직까지 이에 대한 연구가 많지 않은 편이라는 사실을 보여준다 (Dodds et al., 2003). 실제로 현대 기업들의 데이터 네트워크 토폴로지는 흔히 스케일 프리 네트워크(scale-free network)의 특성을 따라가며, 이는 연결성 분포의 측면에서 파워로(power law)를 따른다는 가장 큰 특징을 갖지만, 이러한 특성을 활용한 조직 연구는 많이 찾아볼 수 없는 상황이다 (Albert et al., 2000).

그러나 2000년대에 접어들며 점차 많은 연구가 이러한 특성에 주목하고 있다. 2007년 브라하(Braha)와 바얌(Bar-Yam)은 기업 경영과 같은 복잡한 사회적 현상을 설명하기 위해 복잡계 네트워크의 구조와 기능에 대한 연구가 선행되어야 함을 강조한 바 있다 (Braha et al., 2007). 네트워크의 스케일 프리 구조는 많은 기업들이 제품 아키텍처를 구성하는 데

적용하는 전략들을 반영해줄 가능성이 높기 때문이다 (Braha et al., 1998) . 또한 안드리아니(Andriani)와 멕켈비(McKelvey)는 스케일 프리 이론이 조직내 의사결정, 소비자 판매, 임금, 기업의 크기 및 생태, 그리고 산업 조직 등 수많은 조직 체계에서 찾아볼 수 있는 특성을 띄지만, 아직 그 원인과 결과에 대해서는 많은 것이 밝혀져 있지 않음을 강조하였다 (Andriani et al., 2007).

이렇듯 점차 많은 경영 전략 논문들이 기존의 연구 주제와 네트워크 이론을 접목하는 것은, 이를 통해 기업의 장기적인 성장과 생존에 대한 또 다른 주제와 관점을 발견할 수 있는 까닭이다. 기업들이 보여주는 다양한 스케일 프리 네트워크의 특성에 주목했을 때, 우리는 이 때까지 기술적인 차원의 문제로 인식되어왔던 주제들이 경영자의 전략적인 의사 결정의 대상이 될 수 있음을 발견할 수 있다. 그러한 연장선상에서 본 논문은 기업의 보안 네트워크와 기업의 장기적인 생존과의 관계에 주목하고 있다. 치명적인 손실을 발생시킬 수 있는 기업 네트워크에 대한 보안 침입 문제에 효율적으로 대처하기 위해서 경영자들은 자신의 기업이 따라가고 있는 네트워크의 근본적인 특성을 이해하고 이에 기반한 전략적 의사 결정을 내릴 필요가 있다.

제 2 절 스케일 프리 네트워크의 특성

본 논문에서 주목하는 기업 네트워크의 특성인 스케일 프리 네트워크가 보여주는 특수한 현상을 이해하기 위해서는, 기업의 다양한 네트워크의 특성을 네트워크 이론(network theory)적 관점에서 바라볼 필요가 있다. 네트워크 이론은 기본적으로 노드(node), 그리고 노드와 노드 사이를 이어주는 엣지(edge)의 개념만을 가지고 다양하고 복잡한 시스템에 대한 연구를 가능하게 하며, 노드 및 노드 사이에 어떤 관계를 부여하는가에 따라 무한한 형태의 네트워크가 생성된다. 일례로, 노드를 개별 소비자로 설정하고, 노드를 연결하는 엣지를 소비자 간의 정보 연결로 설정할 경우 우리는 소비자 연결망이라는 네트워크를 구축할 수 있다.

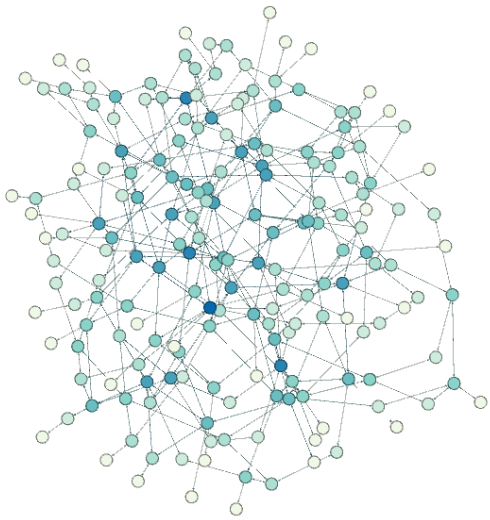
본 논문에서 확인하고자 하는 기업 네트워크를 구축하기 위해서 개별 노드를 각 기업의 서버(server)로, 노드를 잇는 엣지를 서버 사이에서 정보가 오가는 통로로 설정한다. 네트워크 전체를 하나의 산업으로 본다면, 개별 노드를 각 기업으로 설정하고 노드를 연결하는 엣지를 한 기업에서 다른 기업으로 데이터가 전달되는 통로로 설정할 수 있다.

이러한 기업 네트워크는 일반적으로 스케일 프리 네트워크의 특성을 따르는 것으로 알려져 있다. 일반적으로 빈 공간 위에 무작위로 노드들이 존재하고, 각 노드를 다시 무작위로 연결하다보면 가장 기본적인 랜덤 네트워크(random network)가 만들어지는 것으로 알려져 있다. 이러

한 랜덤 네트워크는 시간이 흘러 네트워크가 진화하는 경우에도 개성적인 클러스터(cluster)가 발생하기 쉽지 않으며, 한 노드에서 무작위로 고른 다른 노드를 연결하는 평균 거리, 즉 평균 경로 길이(average path length)가 매우 작다는 특성을 가지고 있다. 만약 기업 네트워크가 랜덤 네트워크를 따른다면, 모든 기업의 정보들은 균등한 정도의 밀도로 서로와 연결되어 있으며 네트워크를 구성하는 어떤 두 노드를 고른다고 하더라도 정보는 똑같은 경로 길이를 거쳐 서로에게 도달할 수 있게 되나, 이는 실제 기업 정보망과 비교했을 때 그다지 현실적이지 않다는 것을 알 수 있다.

이에 착안하여 왓츠(D.J.Watts)가 구성한 네트워크가 바로 스몰 월드 네트워크(small world network)이다 (Watts, 1999). 일반적인 인간 사회를 관찰해 보더라도, 독자적인 개인들이 무작위로 연결되어 있기보다는 지역이나 사전적인 친분에 의해 형성되어 있는 나름대로의 클러스터를 기반으로 관계 맺음을 하게 된다는 것을 알 수 있기 때문이다. 즉, 완전히 독립적이지도 않고 완전히 랜덤하게 흩어져 있지도 않은 중간 단계의 네트워크가 존재하며, 이를 우리는 스몰 월드 네트워크라 부른다. 이러한 스몰 월드 네트워크는 독립적인 노드들로 이루어진 네트워크보다 훨씬 짧게 모든 노드를 관통할 수 있지만 랜덤 네트워크보다는 긴 평균 경로 길이를 가지고 있으며, 대신 랜덤 네트워크가 가지고 있지 않은 높은 수준의 클러스터링(clustering)을 보인다는 독특한 특성을 띤다. 이를 보여주는 간단한 그래프가 바로 [그림 1]이다. 이 스몰 월드 네트워크는 200개

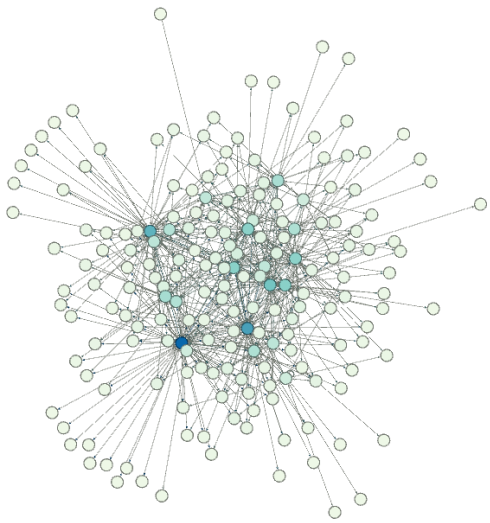
의 노드와 300개의 링크로 구성되어 있으며, 색의 진할수록 더 많은 노드들과 연결되어 있는 높은 연결성(degree)을 가지고 있는 노드라는 사실을 나타낸다. 이를 통해 우리는 각자의 노드가 조금씩 다른 연결성을 보여주고 있으며, 어느 정도 클러스터링이 일어나고 있지만 그 범위가 전반적으로 넓다는 것을 알 수 있다.



[그림 1]

그러나 기업의 데이트 네트워크를 포함하여 인터넷을 기반으로 하는 수많은 네트워크는 스몰 월드 네트워크와는 또 다른 특성을 보여준다. 바로 각 노드들이 다른 노드들과 얼마나 많이 연결되어 있는가를 나타내는 연결성 분포(degree distribution)가 파워로(power-law)를 보인다는 것이며, 이는 스케일 프리 네트워크의 가장 기본적인 성질 중 하나이다. 일반적인 지수함수 형태를 보이는 스몰 월드 네트워크와 스케일 프리 네

트워크의 가장 주요한 두 개의 차이는 바로 성장(growth)과 선호적 연결(preferential attachment)이다 (Barabasi et al., 1999). 정보들의 연결을 핵심적인 성질로 가지고 있는 인터넷 네트워크에서는 보다 많은 정보와 연결되어 있는 노드를 그렇지 않은 노드에 비해 더 선호하게 되며, 이러한 특성을 지니는 노드들이 계속해서 네트워크에 새롭게 유입됨에 따라 [그림 2]에서와 같이 아주 크고 넓은 범위의 네트워크를 아우르는 허브(hub) 역할을 하는 소수의 노드 및 클러스터가 탄생하게 된다.



[그림 2]

이러한 허브의 존재가 본 논문에서 주목하는 기업 네트워크의 보안 침입에 대한 취약성을 발생시키는 근본적인 원인 중 하나가 된다. 인터넷 사이트의 경우를 생각했을 때에도, 한 두 개의 하이퍼링크로 구

성된 사이트가 공격에 처한 경우와 구글과 같은 메가 사이트가 공격에 처한 경우 네트워크 전체의 피해 양상은 확연하게 차이날 수 있음을 직관적으로 알 수 있다. 이렇듯, 스케일 프리 네트워크 및 네트워크의 견고성의 특성을 제대로 파악하지 못한다면 경영자들은 귀중한 기업 정보를 보호하는 데 실패할 수 있으며, 성공한다 하더라도 비교적 값비싼 대가를 치를 수 있는 위험이 존재한다. 이러한 견고성의 특성을 파악하여 의사 결정에 반영할 때 두 가지 종류의 견고성을 모두 이해할 필요가 있으며, 의도적인 공격(targeted attack)에 대한 견고성, 그리고 무작위적인 공격(random attack) 내지 오류(error) 상황에 대한 견고성이 바로 그것이다.

제 3 절 네트워크 아키텍처의 견고성(robustness)

조직의 장기적인 성장을 가능하게 하는 조직의 최적 네트워크 아키텍쳐를 구성하는 것은 많은 경제학자들 및 경영자들의 관심사였으나, 선행 연구의 주된 관심사는 네트워크의 견고성(robustness)보다는 효율성(efficiency)에 있었다 (Williamson, 1975; Sah et al, 1986; Bolton et al., 1994). 그러나 개별 노드를 보호하고, 그 중 일부가 실패한 경우에도 조직 전체가 해체되지 않고 조직으로서 기능하게 하기 위한 견고성은 주목해야 할 특성 중 하나이며 (Dodds et al., 2003), 본 논문에서 중점적으로 관찰하고자 하는 변수이기도 하다.

앞 절에서 간단하게 서술했듯 네트워크의 견고성에는 두 종류가 존재하며, 우연하게 일부의 노드에 발생하는 공격(random attack), 즉 오류(error) 상황에 대한 견고성과, 의도적으로 핵심 노드를 파괴하는 공격(targeted attack)에 대한 견고성이 그것이다 (Albert et al., 2000). 오류는 네트워크를 구성하는 임의의 노드가 기능을 상실하는 것으로, 기업의 데이터 네트워크의 경우 고장, 오작동 등으로 일부 서버가 작동을 정지하거나 데이터가 유실되는 상황 등을 가리킨다. 이를 인사 네트워크의 맥락에서 살펴본다면, 정년 퇴직 혹은 이직 등의 자연적인 이유로 일부 직원들이 퇴사(turnover)하는 상황을 가리킬 수 있다.

반면 공격은 이와 반대로 네트워크를 구성하는 핵심 노드, 즉 가장 많은 연결성을 지니는 허브 역할을 하는 노드를 의도적으로 파괴하거나 마비시켜 기능을 상실케 하는 것을 말한다. 기업 데이터 네트워크의 맥락에 비추어 보면, 이는 본 논문에서 주목하고 있는 보안 침입의 경우를 가리킨다. 외부의 바이러스 공격 등으로 중추 서버가 마비되거나 정보가 유실, 유출되는 상황을 말할 수 있다. 이를 인사 네트워크의 맥락에서 살펴본다면, 한 기업의 핵심적인 기술 및 정보를 보유하고 있는 핵심 인재를 외부에서 빼내어가 인재가 유출되는 상황을 가리킬 수 있다.

이러한 오류와 공격 상황에서의 견고성은 랜덤 네트워크, 스몰 월드 네트워크, 그리고 스케일 프리 네트워크 등 네트워크의 특성에 따라 모두 다르게 나타난다. 스케일 프리 네트워크의 가장 큰 특성 중 하

나가 바로 오류 및 공격 상황에 대한 견고성이 판이하게 다르게 나타난다는 점으로, 이는 제4절에서 보다 상세하게 서술한다.

제 4 절 스케일 프리 네트워크 견고성의 특징

견고성의 측면에서 기업 데이터 네트워크를 포함한 수많은 비즈니스 네트워크가 따라가는 스케일 프리 네트워크는 하나의 중요한 특징을 보인다. 바로 우연하게 발생하는 오류 상황에서는 매우 견고하나, 의도적으로 핵심 노드를 파괴하는 공격 앞에서는 몹시 취약한 특성을 보인다는 것이다 (Albert et al., 2000). 이러한 특징에 주목해야 하는 이유는, 상대적으로 미약한 공격도 기업의 네트워크 전체의 기능성에 큰 영향을 끼칠 수 있으며, 이는 기업 정보 흐름의 효율성 및 커뮤니케이션 능력에 중대한 차질을 미칠 수 있기 때문이다 (Dodds et al, 2003). 그렇게 크지 않은 외부 변화에도 기업의 생존이 크게 위협 받을 수 있는 상황은 장기적인 수익 창출을 목적으로 하는 기업들에는 큰 타격이 될 수 있다. 따라서 이러한 스케일 프리 네트워크의 특성이 왜 발생하는가를 이해하는 것은 경영자들이 이에 대한 대응 전략을 구성하기 위해 무엇보다 중요하다고 할 수 있다.

스케일 프리 네트워크의 가장 큰 특징은 노드와 노드가 비동질적으로(inhomogeneously) 연결된다는 데 있다. 두 노드가 아무런 규칙 없

이 무작위로 연결되는 다른 지수적 네트워크와는 달리, 스케일 프리 네트워크에서 노드는 아무 것에도 연결되지 않은 노드보다 큰 클러스터에 이미 연결되어 있는 노드에 연결되는 것을 더 선호한다. 이 선호적 연결(preferential attachment)에 의해 스케일 프리 네트워크에서 큰 클러스터는 더욱 크고 넓게 번져나갈 수 있게 된다. 바로 이러한 특성 때문에 기업의 데이터 네트워크는 다른 네트워크에 비해 의도적인 공격 앞에서 취약한 모습을 보이게 된다. 의도적인 공격이 몇 개의 핵심 허브를 공격하는 데 성공하기만 한다면, 단 몇 개의 서버가 다운되는 것만으로도 서비스 전체가 마비되는 중대한 이슈가 발생할 수 있는 것이다. 실제로 2016년 말에 발생했던 DNS 업체 Dyn에 대한 Ddos 공격은 약 70여개의 주요 사이트를 대상으로 도합 6시간도 채 지속되지 않았음에도 불구하고, 인터넷 사용자들에게 인터넷 전체가 마비된 것 같은 이용 경험을 줌과 동시에 약 1000억원에 달하는 피해를 끼친 것으로 밝혀졌다 (Burke, 2016).

경영자들은 기업의 장단기적인 생존에 치명적인 영향을 미칠 수 있는 공격 상황에서의 취약성을 극복하기 위해 다양한 방안을 모색할 수 있다. 큰 비용을 들여 공격에 노출될 확률을 낮추는 강력한 보안 업체를 고용할 수도 있고, 자체적으로 새로운 보안 기술을 개발하기 위해 투자를 할 수도 있으며, 그저 기업이 사용하는 보안 시스템을 정기적으로 업그레이드하는 것으로 보안 침입에 대한 대비가 충분하기를 기원할 수도 있다. 그러나 다양한 방법 중에서도 본 논문에서 주목하는 것은, 네트워크 가외성(加外性; redundancy)의 조절을 통해 비교적 직관적이고 효율적

인 방식으로 공격 상황에서의 견고성을 높이는 방안이다.

제 3 장 가 설

제 1 절 네트워크 가외성(redundancy)과 견고성의 상관 관계

네트워크 가외성은 다양한 조직 문헌에서 그 중요성을 주목하기 시작한 개념으로, 조직 행정학적 측면에서 가외성은 여러 기관에 한 가지 기능이 혼합되는 중첩성과 동일 기능이 여러 기관에서 독립적으로 수행되는 독립성을 포괄하는 의미를 말한다. 일반적으로 특정 체계 내에서 구성 요소나 부품의 일부가 필요 이상으로 중복되어 있는 경우 이를 낭비 및 비효율로 생각할 수 있기에 이 때까지의 조직 문헌에서는 가외성이 쓸모없고 불필요한 것으로 인식되었으며, 제거와 개혁의 대상이 되어 왔다.

그러나 최근에 이르러서 가외성이 조직 운영에 있어서 신뢰성과

안정성을 높여주는 순기능을 한다는 주장이 제기되기 시작했다. 불필요한 것처럼 보이는 중첩이 반대로 조직의 토대를 강화시키는 역할을 하여 외부적인 환경 변화가 발생하더라도 그에 큰 영향을 받지 않고 조직의 특성을 유지해나갈 수 있는 중요한 역할을 할 수 있다는 것이다. 이에 따라 오히려 장기적인 조직적 성공을 이끌어내기 위해서는 가외성이 추가적으로 필요하다는 사실이 주목되었다.

비즈니스 네트워크 아키텍처의 견고성의 차원에서도 가외성은 비교적 비용 효율적인 견고성 강화의 방안이 될 수 있다. 이전에는 불필요하다고 인식되었던 데이터 네트워크 내 노드 간의 중첩적인 연결은 비교적 적은 비용을 들여 공격 상황 아래서 값비싼 대가를 치르지 않도록 해주는 효과적인 방안이 될 수 있다.

제 2 절 가설 제시

이를 확인하기 위해서는 네트워크 내에서 가외성이 추가될 때마다 네트워크의 주요한 특성이 어떻게 변화해나가는가를 관찰할 필요가 있다. 이 때, 일반적으로 정보의 흐름을 생명으로 하는 네트워크에서 주목해서 관찰해야 할 변수는 바로 평균 경로 길이(average path length)와 최대 클러스터의 크기(size of the largest cluster)로 알려져 있다. 평균 경로 길이는 네트워크 내에서 무작위의 두 개의 노드를 선택했을 때 그 노드 간

의 평균 거리가 얼마인지를 나타내는 개념으로, 네트워크 상의 정보가 얼마나 빠르고 효율적으로 전달될 수 있는가를 나타내는 척도이다. 평균 경로 길이가 짧은 네트워크는 정보가 신속하게 도달할 수 있으며, 반대로 평균 경로 길이가 긴 네트워크는 정보가 더디게 도착한다. 이에 비추어 보았을 때, 우리는 의도적인 공격 상황 아래에서 스케일 프리 네트워크의 특성을 보이는 기업 네트워크는 핵심 노드들에 공격에 처함에 따라 빠른 속도로 평균 경로 길이가 늘어날 것이라는 점을 알 수 있다. 본 논문에서 검증하고자 하는 첫 가설은 바로 네트워크에 가외성이 추가될수록 평균 경로 거리의 증가 속도가 더뎌질 것이라는 것이다. 똑같은 핵심 허브에 대한 공격이 발생한다 하더라도, 가외성이 강해진 네트워크에서는 정보가 전달되는 속도가 보다 오랫동안 강하게 유지될 수 있다면 기업이 이를 통해 입게 되는 직간접적인 손실의 크기는 대폭 축소될 수 있다.

가설 1a. 네트워크 가외성이 강해질수록 공격에 의한 기업 네트워크의 평균 경로 길이의 손상이 약화될 것이다.

네트워크의 주요 특성을 나타내는 두 번째 변수는 바로 최대 클러스터의 크기로, 이는 네트워크의 전반적인 회복력(resilience)을 보여주는 척도이다. 스케일 프리 네트워크는 주요 허브들을 중심으로 크고 작은 클러스터를 형성하고 있기 때문에, 그 중 가장 커다란 클러스터가 공

격 상황 아래에서 얼마나 오랫동안 유지되는가는 매우 중요한 이슈이다. 빠른 시간 안에 전 네트워크의 중추 역할을 하는 최대 클러스터가 붕괴될 경우 공격이 끝난 이후에 정보망을 회복하는 데 큰 비용이 들 수 밖에 없기 때문이다. 스케일 프리 네트워크의 특성을 따라가는 기업 네트워크는 핵심 노드를 중심적으로 공격하는 의도적인 공격 상황 아래에서 빠른 속도로 최대 클러스터가 해체되어 갈 것이나, 본 논문에서는 가외성의 추가가 효율적으로 이 속도를 늦춰줄 수 있는 기제가 될 수 있음을 가정한다.

가설 1b. 네트워크 가외성이 강해질수록 공격에 의한 기업 네트워크의 회복력의 손상이 약화될 것이다.

그러나 이것이 정말 기업에게 비용 효율적인 방안이 될 수 있는가를 검증하기 위해서는 불필요한 중첩, 즉 가외성의 강화로 인해 기존의 기업 네트워크가 가지는 가장 큰 강점 중 하나인 랜덤 공격 혹은 오류 상황 아래에서의 강력한 견고성이 희생되지 않는가를 살펴볼 필요가 있다. 만약 공격 상황에서의 견고성의 강화가 오류 상황에서의 강한 견고성을 담보로 한 것이라면, 기업의 입장에서는 더 큰 비용을 지불할 위험이 뒤따르게 된다. 그러나 가외성이 강화된 네트워크라고 하더라도 기존의 스케일 프리 네트워크가 보여주는 파워로 분포의 특성에는 변함이 없을 것이기 때문에, 무작위로 노드를 공격하는 오류 상황 아래에서 기

존의 네트워크가 보여주는 강력한 견고성에는 변화가 없을 것이라고 가정할 수 있다.

가설 2a. 네트워크 가외성이 강해진다고 해도 오류에 의한 기업 네트워크의 평균 경로 길이의 견고성에는 변화가 없을 것이다.

가설 2b. 네트워크 가외성이 강해진다고 해도 오류에 의한 기업 네트워크의 회복력의 견고성에는 변화가 없을 것이다.

제 4 장 연구 방법

제 1 절 시뮬레이션 연구 방법론

네트워크 가외성이 오류와 공격 상황 아래에서의 비즈니스 네트워크의 견고성에 미치는 영향을 알아보기 위해 본 연구에서 채택한 연구 방법은 시뮬레이션 연구 방법론이다. 시뮬레이션 연구방법론은 스케일 프리 네트워크를 구성하는 기본적인 알고리즘을 구성한 이후, 임의로 무작위의 노드를 골라 파괴하는 오류 상황과 가장 연결성이 높은 핵심 노드부터 제거하는 공격 상황을 조작하여 이에 따라 네트워크가 얼마나 견고하게 대응하는가를 살펴볼 수 있는 효과적인 방법이다.

가외성을 추가하는 데에도 여러 가지 방식이 존재하는 것으로 알려져 있으나, 본 논문에서는 홀메(P. Holme)와 김(B. J. Kim)이 제안한 트라이어드 형성(triad formation)의 방식을 사용한다 (Holme et al., 2002). 트라이어드 형성은 하나의 신규 노드가 기존의 노드들에 선호적 연결을 한 이후, 특정 확률에 따라 연결한 기존의 노드와 연결되어 있는 또 다른 노드와도 연결을 함으로써 트라이어드(triad)를 형성하는 형태로 네트워크를 구성하는 방식을 말한다. 이를 통해 우리는 서버 네트워크 등을 구축하는 경우 자연스럽게 발생하는 선호적 연결 이외에도, 임의의 또 다른 서버와의 의도적이고 중첩적인 연결을 추가해줌으로써 네트워크의 가외성을 강화시킬 수 있다.

이를 구현하기 위해 구성하는 초기 조건(initial condition)은 다음과 같다. 사용하는 노드의 총 개수 **n**은 10,000개이며 우선 연결성이 없는, 즉 엣지(edge)의 개수가 0이고 m_0개의 노드(node)가 존재하는 네트워크를 코딩한다. 이후 스케일 프리 네트워크의 핵심적인 알고리즘인 성장(growth)을 구현하기 위해 매 **t**기마다 네트워크에 **m**개의 엣지를 갖는 새로운 노드 **v**를 등장시킨다.

그 다음으로 스케일 프리 네트워크의 가장 큰 특징인 선호적 연결(preferential attachment)을 구성하기 위해, 노드 **v**가 $\mathbf{k_v}$개의 이웃 노드를 가지고 있다고 했을 때 $P_w = \frac{k_w}{\sum_{v \in V} k_v}$ 의 확률로 기존에 존재하는 노드 **w**를 고르게 한다. 즉, 이웃이 많은 노드일수록 더 높은 확률로 트라이아드 형성을 시도하게 된다는 것이다.

이후 공격과 오류의 알고리즘을 각각 구현하여, 각 상황 아래에서 평균 경로 길이와 네트워크의 회복력의 두 가지 요소가 어떻게 변화해가는가를 관찰하는 것이 본 논문의 목적이다.

제 2 절 독립 변수

본 논문에서 조절하고자 하는 독립변수에는 두 가지가 있다. 첫 번째는 바로 가외성 강화를 시도하는 횟수, 즉 $m_t = (m-1)P_t$이다. 이 때 $(m-1)$은 기존의 선호적 연결 이외의 연결, 즉 트라이어드 형성의 횟수를 나타내는 것이며, P_t는 매기 트라이어드 형성을 시도할 확률을 나타내는 것이다. 홀메의 트라이어드 형성을 통한 가외성 강화의 장점은 바로 이 m과 P_t의 조절을 통해 가외성의 강화 정도를 변화시켜가며 효과를 살필 수 있다는 점이다. 본 논문에서는 매 t기마다 트라이어드가 일어나도록 설정하기 위해 P_t = 1 로 설정하였으며, 트라이어드 형성의 횟수, 즉 m을 각각 1, 2, 3의 순으로 변화해가며 가외성 강화의 강도를 높이는 방식을 사용하였다.

두 번째 독립변수는 바로 공격 및 오류의 횟수이다. 공격 상황을 구현하기 위해서는 네트워크의 성장이 모두 끝난 이후 가장 이웃 노드가 많은 노드, 즉 핵심 허브 역할을 하는 노드부터 순차적으로 제거한다. 반

면, 오류 상황의 경우 어떠한 조건도 없이 존재하는 모든 노드를 같은 확률 아래서 무작위로 선택하여 제거하는 알고리즘을 사용한다. 이들 각각을 연속적으로 실행시키면서 이에 따른 종속 변수의 변화를 살펴봄으로써 가외성의 강화가 공격 및 오류 상황에서의 견고성에 어떠한 영향을 미치는가를 확인할 수 있다.

제 3 절 종속 변수

이를 통해 본 연구에서 살피고자 하는 종속 변수는 네트워크의 평균 경로 길이(average path length)와 네트워크의 회복력(resilience), 즉 최대 클러스터의 상대적인 크기(relative size of the largest cluster)이다.

한 노드가 무작위로 고른 다른 노드까지 도달하기까지 걸리는 평균적인 거리를 나타내는 평균 경로 길이가 작을수록 한 노드에 퍼진 정보는 더욱 빠른 속도로 네트워크 전체에 퍼져나갈 수 있기 때문에, 효율적인 네트워크임을 나타내는 척도로 작용할 수 있다. 또한, 공격 및 오류에 의해 노드가 없어질 때 직경의 변화가 그리 크지 않다면, 우리는 그 네트워크의 안전성이 높다고 판단할 수 있다. 반대로 노드가 제거될 때마다 직경의 크기가 크게 변동한다면, 우리는 그 네트워크의 안전성에 의문을 제기할 수 있다.

두 번째 종속 변수는 네트워크의 회복력, 즉 가장 큰 클러스터의

상대적 크기의 변화이다. 네트워크 전체의 크기를 1로 놓고, 네트워크 진화가 모두 끝난 후 형성된 가장 큰 클러스터의 크기를 1에 대한 상대적인 비율로 표시한다. 이후 공격 및 오류 상황에 의거하여 노드를 제거함에 따라 변화되는 클러스터의 크기를 계속해서 상대적으로 표시한다. 공격 상황 아래에서 노드가 지속적으로 제거되어도 가장 클러스터의 크기가 지속적으로 유지된다면 네트워크의 중추로서의 기능을 쉽게 상실하지 않는 강한 회복력을 의미한다.

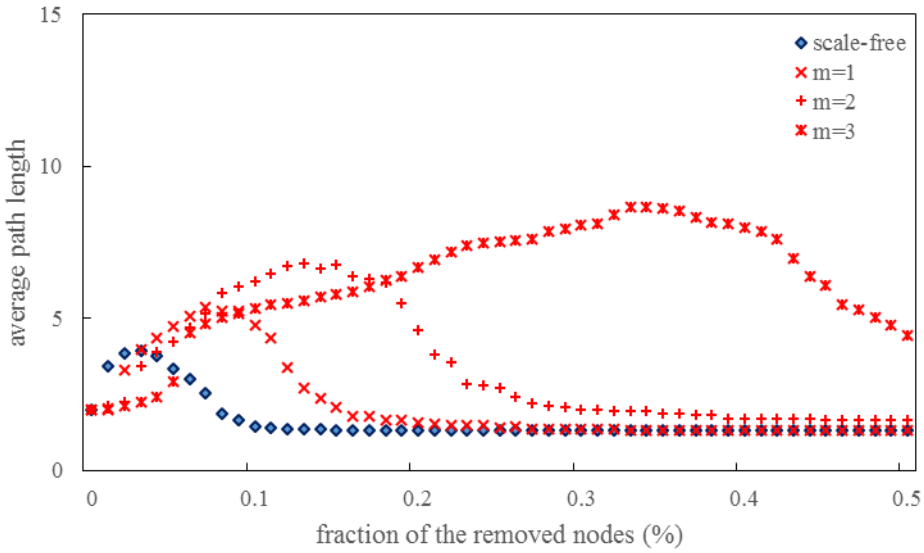
제 5 장 연구 결과

제 1 절 종속 변수 1: 평균 경로 길이

기업 네트워크의 공격 상황 아래서의 평균 경로 길이의 변화를 그래프로 나타낸 것이 [표 1 - 1]이다. 가로축은 전체 노드 중에서 공격을 통해 제거한 노드의 개수의 비율을 퍼센테이지(%)로 나타낸 것이며, 세로축은 평균 경로 길이를 나타낸 것이다. 가외성을 강화하지 않은 상황과 가외성을 점차 추가해나가는 상황 모두 평균 경로 길이가 증가하다가 다시 감소하는 추세를 보임을 발견할 수 있는데, 이는 최대 클러스터가

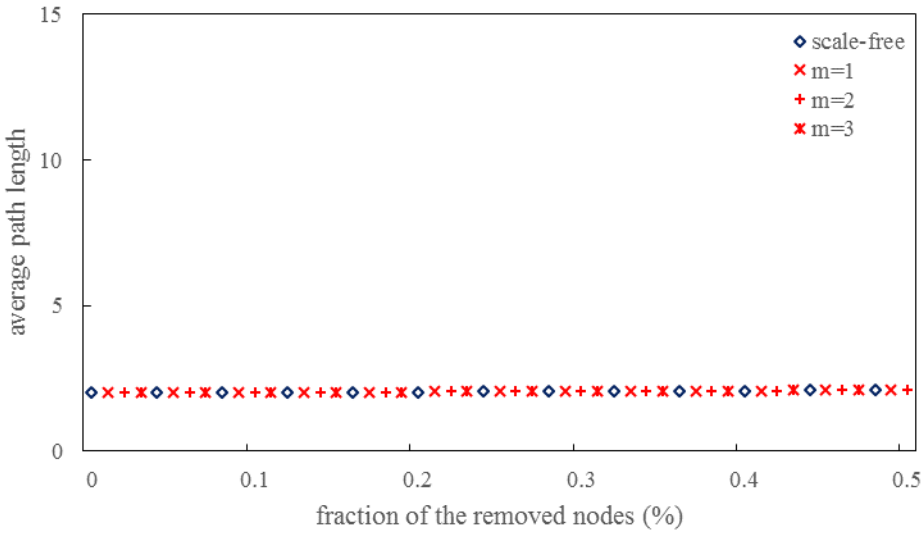
붕괴되는 시점을 기준으로 발생하는 현상으로 설명할 수 있다. 최대 클러스터가 붕괴되어감에 따라 평균 경로 길이가 점차 길어지고, 최대 클러스터가 소멸되는 시점을 기준으로 네트워크의 전체적인 규모가 급격히 작아지면서 평균 경로 길이가 그에 맞춰 줄어들게 되는 것이다.

푸른색 다이아몬드로 표시된 것이 가외성을 강화하지 않은 기존의 기업 네트워크의 평균 경로 길이의 변화이다. 가장 많은 노드들과 연결되어 있는 핵심 노드부터 파괴하는 공격 상황 아래에서, 기존의 기업 네트워크의 평균 경로 길이는 급격하게 증가하다 0.3%의 노드가 없어지는 시점에서 최대 클러스터의 붕괴와 함께 줄어들게 된다.



[표 1 - 1]

가외성 강화가 시행된 경우는 붉은 색으로 표시했으며, 강화의 정도에 따라 각기 다른 표식을 사용하였다. 약한 가외성 강화, 즉 m = 1 일 경우 평균 경로 길이는 가외성이 전혀 추가되지 않은 기업 네트워크에 비해 확연히 완만한 속도로 평균 경로 길이가 증가한다는 것을 알 수 있다. 0.15%의 노드가 제거되는 시점을 기준으로 최대 클러스터가 붕괴되며 다시 평균 경로 길이가 증가하는데 m의 크기, 즉 가외성의 강화 정도가 커짐에 따라 평균 경로 길이가 증가하는 속도가 점차 느려진다는 것을 확인할 수 있다.



[표 1 - 2]

우리는 이를 통해 약한 가외성 추가 매커니즘을 통해서도 공격에 대한 견고성을 비교적 단순하게 제고할 수 있다는 사실을 알 수 있으며, 이를 통해 가설 1a을 검증할 수 있다. 가외성이 추가되면서 견고성의 효과는 점차 증폭되어 나타나며, 이를 통해 네트워크 안전성이 한층 강화되는 효과를 보여준다.

그러나 이러한 공격 상황에서의 견고성의 강화는 오류 상황에서의 견고성 약화를 동반해서는 안 된다. [표 1 – 2]는 오류 상황에서의 평균 경로 길이를 나타낸 것으로, 계속해서 가외성을 강화해나간다 하더라도 무작위로 일부 노드가 작동을 멈추는 경우 평균 경로 길이는 거의 변함이 없음을 보여준다. 이는 가외성이 추가된 경우에도 기업 네트워크가 계속해서 스케일 프리 네트워크의 특성을 따름을 나타낸다. 우리는 이를 통해 가설 2a를 검증할 수 있다.

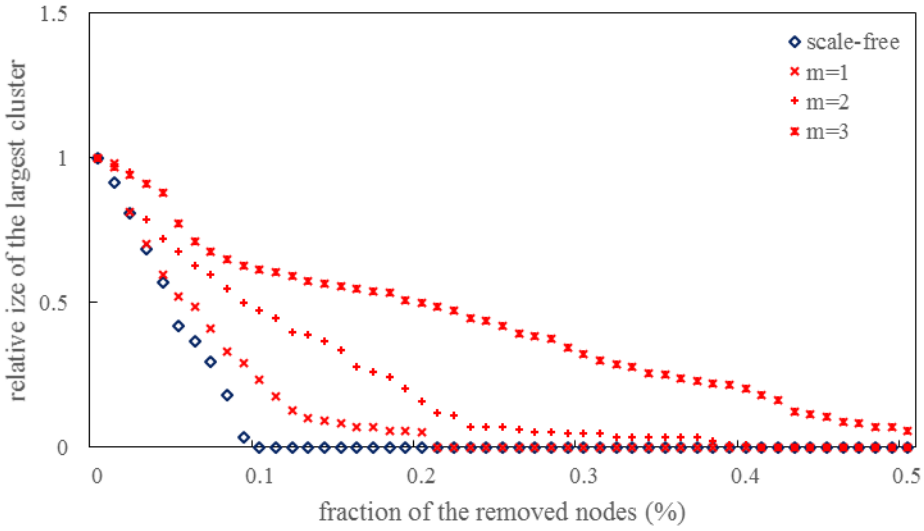
제 2 절 종속 변수 2: 최대 클러스터 크기

두 번째 연구 결과는 공격 및 오류 상황 아래에서의 네트워크의 회복력, 즉 최대 클러스터의 상대적 크기의 변화를 나타낸 것이다. [표 2 – 1]와 [표 2 – 2]는 각기 공격과 오류의 상황을 표시한 것이다.

공격 상황 아래서 푸른색 다이아몬드로 표현된 기존의 기업 네

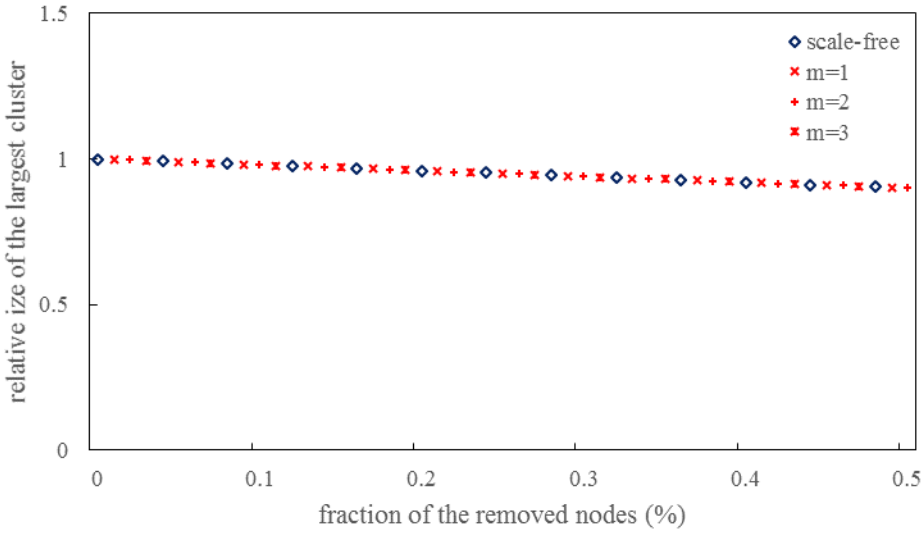
트워크는 0.1%의 핵심 노드가 제거되는 것으로 최대 클러스터가 모두 소멸되는 모습을 보인다. 즉, 기업의 핵심 서버 몇 개를 마비시키는 것만으로도 네트워크의 중추 역할을 하는 정보망이 전체적으로 중단되는 사태에 이를 수 있는 취약한 구조를 보이고 있다.

그러나 붉은 색으로 표시된 가외성이 강화된 네트워크 하에서는 최대 클러스터가 소멸되는 시점이 점차 늦춰지고 있음을 알 수 있다. m = 1, 즉 약한 가외성의 상황에서도 최대 클러스터가 소멸되는 시점은 2배 가까이 늘어나며, m = 2인 경우에는 4배까지 늘어난다. 또한 m = 3의 강한 가외성의 네트워크는 좀처럼 최대 클러스터가 소멸되지 않는 견고한 모습을 보여준다는 것을 알 수 있다. 이러한 경우 Ddos 공격 등으로 기업의 핵심 서버가 마비되거나 산업의 핵심 기업들의 사이트가 마비되는 경우에도 전체적인 네트워크는 네트워크로서의 기능을 계속해서 수행할 수 있으며, 공격이 중단된 이후의 회복에도 큰 차질 없이 복귀할 가능성이 높아지게 된다. 비교적 간단한 가외성 강화라는 방법을 통해 기업이 막을 수 있는 경제적인 손실의 액수는 천문학적인 액수에 달할 수 있다는 점에서, 이는 주목해야 할 결과라고 할 수 있으며, 이를 통해 가설 1b를 검증할 수 있다.



[표 2 - 1]

그러나 이 결과 역시 기존 기업 네트워크의 오류 상황에서의 강한 견고성을 담보로 하는 것이라면 오히려 기업의 입장에서는 생각지도 못한 어려움을 겪게 될 수 있다. 오류 상황에서의 회복력의 견고성이 약화될 경우 치명적인 영향을 줘서는 안 되는 간단한 일부 서버의 고장에도 전체 네트워크의 중추에 큰 타격을 입을 수 있기 때문이다.



[표 2 - 2]

이를 확인하기 위해 오류 상황에서의 최대 클러스터의 상대적인 크기의 변화를 나타낸 것이 [표 2 – 2]로, 오류가 계속해서 발생하더라도 최대 클러스터의 상대적 크기는 비교적 견고하게 유지되고 있음을 확인할 수 있다. 가외성에 강화된다고 해도 회복력의 견고한 정도는 변함없이 유지되고 있다는 점에서, 가설 2b 또한 성립한다는 것을 확인할 수 있다.

이를 통해 트라이어드 형성을 통한 가외성 강화의 방식이 오류 상황에서의 강한 견고성은 그대로 유지하면서 공격 상황에서의 취약성을 크게 보강해줄 수 있음을 확인할 수 있다. 또한 가외성 강화의 정도가 증가함에 따라 그 효과가 점점 강해진다는 사실 또한 확인할 수 있다.

제 6 장 토의 및 결론

기업들의 인터넷 의존도가 높아짐에 다라 기업 네트워크를 견고하게 구성하는 것의 중요성은 더욱 커지고 있으나, 기업의 네트워크 서비스가 외부의 공격에 특히 취약한 메커니즘에 대한 연구는 많지 않았던 것이 사실이다. 이에 대한 인식의 부재는 갈수록 많은 기업들이 자체적인 네트워크를 구성하고 그에 대한 서비스 의존도를 강화하는 현 시점에 더욱 큰 문제를 초래할 수 있는 위험성을 가지고 있다. 일례로 잠재적인 성장성이 클 것으로 예측되는 커넥티드 카 시장에서 기업들은 자체적인 클라우딩 컴퓨팅 네트워크 상에 소비자의 안전과 생명과 직결되는 수많은 정보들을 보유하게 되는데, 핵심 허브에 대한 공격에 취약한 기업 네트워크에 대한 전략을 적절하게 구상하지 않았을 때 기업 및 소비자가 입게 되는 피해의 규모는 천문학적인 액수에 달할 수 있다. 이에 본 논문에서는 트라이어드 형성의 가미라는 비교적 단순한 장치를 설정하는 것으로 기업들이 자신의 네트워크 서비스의 오류 상황에서의 높은 견고성을 낮추는 희생을 하지 않고도, 공격 상황에서의 견고성을 높일 수 있다는 점을 강조하고 있다.

그러나 본 논문에서 사용한 방식은 네트워크 가외성을 추가할 수 있는 하나의 대표적인 메커니즘으로, 또 다른 방식으로 가외성을 추가할 경우 네트워크 견고성은 어떻게 변화할지를 알아보는 것은 의미 있는 향후 연구의 주제가 될 수 있다. 나아가 실제 기업 네트워크에서는

대부분의 경우 한없이 성장하기만 하는 것이 아니라, 노후한 연결고리는 삭제되고 새로운 정보망은 더욱 강화되는 등의 변화가 생긴다는 점에 착안하여 (Klemm et al., 2002), 이를 반영한 네트워크 상에서의 가외성 강화의 효과를 살펴보는 것 또한 의미 있을 것이다.

또한, 스케일 프리 네트워크가 아닌 상이한 네트워크 토폴로지 하에서 가외성의 추가가 견고성에 어떠한 영향을 미치는가를 살펴보는 것 또한 의미 있는 연구가 될 수 있다. 스케일 프리 네트워크와 함께 기업 조직에서 가장 많이 발견할 수 있는 또 다른 토폴로지가 바로 이전의 절에서 서술한 스몰 월드 네트워크이다. 이는 스케일 프리 네트워크의 연결성 분포가 파워로를 따르는 것과 달리, 지수적 연결 분포를 보이며 인사 조직 구성 및 커뮤니케이션 시스템이 대표적으로 스몰 월드 네트워크를 따라가는 것으로 알려져 있다 (Dodds et al., 2003). 조직 내 퇴사 및 이직 문제는 조직의 지식을 보존하고 유지하는 데 핵심적인 주제라 할 수 있는데, 본 논문에서 주목하는 견고성의 측면에서 자연스럽게 조직 구성원이 퇴직하는 것을 오류, 외부에서 핵심 조직 구성원을 빼내어가는 상황을 공격이라고 볼 수 있다. 따라서 조직 체계 내에 가외성을 추가했을 경우 인사 조직과 같은 스몰 월드 네트워크의 견고성이 어떻게 변화하는가를 살펴볼 수 있다면, 우리는 조직의 구성에 관한 새로운 통찰을 얻을 수 있을 것이다.

마지막으로, 본 논문은 기업들이 의존하는 네트워크의 본질적인 특성에 의거하여 견고성을 높일 수 있는 하나의 메커니즘을 제시하고 있

다는 점에서 전략 문헌이 보다 다양한 관점에서 기업의 네트워크를 다루는 데 기여하고 있다. 본 논문에서 사용한 시뮬레이션 연구방법론 또한 아직 전략 문헌에서 많이 쓰이고 있지 않으나, 기존의 연구방법론과는 또 다른 시각에서 다양한 주제를 실험할 수 있는 기회가 될 수 있다. 이는 2000년대 후반을 기점으로 다양한 전략 학술지에서 스케일 프리 네트워크의 특성에 주목하여 그와 관련된 연구를 확대하고 있는 추세와도 맞닿아 있다고 할 수 있다.

참고 문헌

1. Albert, R. & Jeong, H. & Barabasi, A. L. Error and attack tolerance of complex networks. *Nature* **406**, 378-382 (2000).

2. Andriani, P. and McKelvey, B. From Gaussian to Paretian Thinking: Causes and Implications of Power Laws in Organizations. *Organization Science* **20(6)**, 1053–1071 (2007).

3. Barabasi, A.-L. & Albert, R. Emergence of scaling in random networks. *Science* **286**, 509-511 (1999).

4. Bolton, P. & Dewatripont, M. The Firm as a Communication Network. *The Quarterly Journal of Economics* **109** 809-839 (1994)

5. Braha, D. & Bar-Yam, Y. The Statistical Mechanics of Complex Product Development: Empirical and Analytical Results. *Management Science* **53(7)**, 1127-1145 (2007).

6. Braha, D. & Maimon, O. A Mathematical Theory of Design: Foundations, Algorithms, and Applications. Kluwer Academic Publishers, Boston, MA (1998).

7. Campbell, K. & Gordon, L. A. & Loeb, M. P. & Zhou, L. The Economic Cost of Publicly Announced Information Security Breaches: Empirical

Evidence from the Stock Market. *Journal of Computer Security* **11**, 431-448 (2003).

8. Cashell, B. & Jackson, W. D. & Webel, B. The Economic Impact of Cyber-Attacks. *CRS Report for Congress* (2004)

9. Cavusoglu, H. & Mishra, B. & Raghunathan, S. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce* **9(1)** 70-104 (2004)

10. Cohen, R. & Havlinn S. & Ben-Avraham, K. D. Efficient immunization strategies for computer networks and populations. *Physical Review Letters* **91**, 247901 (2009).

11. Dodds, P. S. & D. J. Watts & C. F. Sabel. Information exchange and the robustness of organizational networks. *Proceedings of the National Academy of Science.* USA 100 12516–12521 (2003).

12. Faloutsos, M., Faloutsos, P. & Faloutsos, C. *Computational Communication Review* **29**, 251–262 (1999).

13. Gerth, H. H. & Mills, C. W., eds. From Max Weber: Essays in Sociology, Oxford University Press, New York (1946)

14. Glober, S. & Liddle, S. & Prawitt, D. Electronic Commerce: Security, Risk

Management, and Control. Upper Saddle River. NJ: Prentice Hall (2001)

15. Guimera, R. & Uzzi, B. & Spriro, J. & Amaral, L. A. N. Team assembly mechanisms determine collaboration structure and team performance. *Science* **308**, 697-702 (2009).

16. Holland, J. H. Complex adaptive systems and spontaneous emergence. A. Q. Curzio, M. Fortis, eds. Complexity and Industrial Clusters. *Physica-Verlag*, Heidelberg, Germany, 24–34 (2002).

17. Holme, P. & Kim, B. Growing scale-free networks with tunable clustering. *Physical Review E* **65**, 026107 (2002).

18. Hovav, A., D'Arcy, J. The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review* **6(2)**, 97-121 (2003).

19. Java, A. & Finin, T. & Song, X. & Tseng, B. Why We Twitter: Understanding Microblogging Usage and Communities. *Proceedings of the 9th WebKDD and 1st SNA-KDD 2007 workshop on Web mining and social network analysis*, 56-65 (2007).

20. Kannan, K. & Rees, J. & Sridhar, S. Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce* **12(1)** 69-91 (2007)

21. Klemm, K. & Eguiluz, V. M. Highly Clustered Scale-free Networks. *Physical Review E* **65** 036123 (2002).

22. Nishiguchi, T. & Beaudet, A. In Knowledge Creation: A New Source of Value, eds. Von Krogh, G., Nonaka, I. & Nishiguchi, T. (MacMillan, London), 199–230 (2000).

23. Ponemon Institute LLC. 2014 Cost of Data Breach Study: Global Analysis (2014)

24. Sah, R. K. & Stiglitz, J. E. The Architecture of Economic Systems: Hierarchies and Polyarchies. *The American Economic Review* **76(4)** 716-727 (1986)

25. Salierno, D. Managers Fail to Address E-Risk. *The Internal Auditor*. April, 13 (2001)

26. Streeter, L.A., Kraut, R.E., Lucas, H.C. & Caby, L. How Open Data Networks Influence Business Performance and Market Structure. *Communications of the ACM* 39(7), 63-73 (1996).

27. Strogatz, S. H. Exploring complex networks. *Nature* **401**, 268-276 (2001).

28. Van Zandt, T. Organizations with Incomplete Information, Cambridge University Press, New York, 239–305 (1998).

29. Warren, M. & Hutchinson, W. Cyber Attacks Against Supply Chain

Management Systems: A Short Note. *International Journal of Physical Distribution & Logistics Management* **30(6)** 710-716 (2000)

30. Watts, D. J. Networks, dynamics, and small world phenomenon. *American Journal of Sociology* **105**, 493-527 (1999).

31. Williamson, O. E. Markets and Hierarchies: Analysis and Antitrust Implications, Free Press, New York, (1975).

Abstract

The Effects of Network Redundancy on the Resilience of Business Network: Focusing on the Firm Data Network

DaUn Jung
Business School
Strategy and International Management
The Graduate School
Seoul National University

The purpose of this study is to investigate the strategy to strengthen the network resilience in order to protect corporate information assets from network attacks. Strategic decisions to manage and protect data networks are crucial to securing long-term performance of business firms. However, the data network of contemporary business firms shows extremely weak robustness under external attacks, which leads to major financial losses even under minor attacks. By using simulation computational method, this study shows that by adding rather small amount of redundancy, firms can efficiently strengthen the resilience of the business

network.

Keywords : business network, network redundancy, network resilience
Student Number : 2015-20666